

Translation

PATENT COOPERATION TREATY

PCT/JP2003/013772



PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P0648PC	FOR FURTHER ACTION	See Form PCT/IPEA/416
International application No. PCT/JP2003/013772	International filing date (day/month/year) 28 October 2003 (28.10.2003)	Priority date (day/month/year) 30 October 2002 (30.10.2002)
International Patent Classification (IPC) or national classification and IPC H04N 1/387		
Applicant JAPAN SCIENCE AND TECHNOLOGY AGENCY		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets, including this cover sheet.

3. This report is also accompanied by ANNEXES, comprising:

a. ☒ (sent to the applicant and to the International Bureau) a total of 12 sheets, as follows:

☒ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).

☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.

b. ☐ (sent to the International Bureau only) a total of (indicate type and number of electronic carrier(s)) _____, containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

☒ Box No. I Basis of the report

☐ Box No. II Priority

☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

☐ Box No. IV Lack of unity of invention

☒ Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

☐ Box No. VI Certain documents cited

☐ Box No. VII Certain defects in the international application

☐ Box No. VIII Certain observations on the international application

Date of submission of the demand 26 May 2004 (26.05.2004)	Date of completion of this report 18 November 2004 (18.11.2004)
Name and mailing address of the IPEA/JP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.

PCT/JP2003/013772

Box No. I Basis of the report

1. With regard to the language, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

- ☐ This report is based on translations from the original language into the following language _____, which is language of a translation furnished for the purpose of:
- ☐ international search (under Rules 12.3 and 23.1(b))
- ☐ publication of the international application (under Rule 12.4)
- ☐ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the elements of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

- ☐ The international application as originally filed/furnished
- ☒ the description:
- pages _____ 1-26 _____, as originally filed/furnished
- pages* _____ received by this Authority on _____
- pages* _____ received by this Authority on _____
- ☒ the claims:
- pages _____ 4-14 _____, as originally filed/furnished
- pages* _____, as amended (together with any statement) under Article 19
- pages* 1-3, 15-20 received by this Authority on 26 May 2004 (26.05.2004)
- pages* _____ received by this Authority on _____
- ☒ the drawings:
- pages _____ 1-13 _____, as originally filed/furnished
- pages* _____ received by this Authority on _____
- pages* _____ received by this Authority on _____
- ☐ a sequence listing and/or any related table(s) – see Supplemental Box Relating to Sequence Listing.

3. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/figs _____
- ☐ the sequence listing (*specify*): _____
- ☐ any table(s) related to sequence listing (*specify*): _____

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/figs _____
- ☐ the sequence listing (*specify*): _____
- ☐ any table(s) related to sequence listing (*specify*): _____

* If item 4 applies, some or all of those sheets may be marked "superseded."

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP 03/13772

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-20	YES
	Claims		NO
Inventive step (IS)	Claims	1-20	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-20	YES
	Claims		NO

2. Citations and explanations

Document 1: Hideaki Tamori et al., "Suuron Henkan wo Mochiita Kaizan Kenshutsu Kanou na Denshi Sukashi Houshiki", The Institute of Electronics, Information and Communication Engineers Gijutsu Kenkyuu Houkoku, IE2001-33, 1 July 2001, pages 105 to 110

Document 2: Hideako Tamori et al., "Suuron Henkan ni yoru Zeijakugata Denshi Sukashi wo Mochiita Seishi Gazou no Kaizan Ichi Kenshutsu Kanou to Kaizan Teisei", The Institute of Electronics, Information and Communication Engineers Gijutsu Kenkyuu Houkoku, IE2002-45, 1 July 2002, pages 19 to 24

Neither document 1 nor document 2 cited in the international search report discloses or indicates that the embedment value is determined from the number theoretic transform block of the original image block of the embedment position, the pixel value of the signature image, and the embedment strength, or that the extraction position which corresponds to the embedment position of the signature image is determined based on the randomizing function with information concerning surrounding predetermined blocks as parameters, and said features

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP 03/13772

would not be obvious to a person skilled in the art.

Therefore the invention set forth in claims 1 to 20
is novel and involves an inventive step.

特 許 協 力 条 約

発信人 日本国特許庁（国際予備審査機関）

出願人代理人 橋爪 健 様 あて名 〒 104-0061 東京都中央区銀座3丁目13番17号		PCT 特許性に関する国際予備報告（特許協力条約第二章）の 送付の通知書 （法施行規則第57条） [PCT規則71.1]	
出願人又は代理人 の書類記号 P0648PC		発送日 （日.月.年） 14.12.2004	
国際出願番号 PCT/JPO3/13772	国際出願日 （日.月.年） 28.10.03	優先日 （日.月.年） 30.10.02	
出願人（氏名又は名称） 独立行政法人科学技術振興機構			
1. 国際予備審査機関は、この国際出願に関して特許性に関する国際予備報告及び付属書類が作成されている場合には、それらをこの送付書とともに送付することを、出願人に通知する。 2. 国際予備報告及び付属書類が作成されている場合には、すべての選択官庁に通知するために、それらの写しを国際事務局に送付する。 3. 選択官庁から要求があったときは、国際事務局は国際予備報告（付属書類を除く）の英語の翻訳文を作成し、それをその選択官庁に送付する。 4. 注 意 出願人は、各選択官庁に対し優先日から30月以内に（官庁によってはもっと遅く）所定の手続（翻訳文の提出及び国内手数料の支払い）をしなければならない（PCT39条（1））（様式PCT/IB/301とともに国際事務局から送付された注を参照）。 国際出願の翻訳文が選択官庁に提出された場合には、その翻訳文は、国際予備審査報告の付属書類の翻訳文を含まなければならない。この翻訳文を作成し、関係する選択官庁に直接送付するのは出願人の責任である。 選択官庁が適用する期間及び要件の詳細については、PCT出願人の手引き第Ⅱ巻を参照すること。 出願人はPCT第33条(5)に注意する。すなわち、PCT第33条(2)から(4)までに規定する新規性、進歩性及び産業上利用可能性の基準は国際予備審査にのみ用いるものであり、締約国は、請求の範囲に記載されている発明が自国において特許を受けることができる発明であるかどうかを決定するに当たっては、追加の又は異なる基準を適用することができる（PCT第27条(5)も併せて参照）。そのような追加の基準は、例えば、実施可能要件や特許請求の範囲の明確性又は裏付け要件を、特許要件から免除することも含む。			

名称及びあて名 日本国特許庁（IPEA/JP） 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	権限のある職員 特 許 庁 長 官 電話番号 03-3581-1101 内線 3571	5V 3359
---	---	---------

Rec'd 18 APR 2005

特 許 協 力 条 約

PCT

REC'D 16 DEC 2004

WIPO

PCT

特許性に関する国際予備報告 (特許協力条約第二章)

(法第12条、法施行規則第56条)
[PCT36条及びPCT規則70]

出願人又は代理人 の書類記号 P 0 6 4 8 P C	今後の手続きについては、様式PCT/IPEA/416を参照すること。	
国際出願番号 PCT/J P 0 3 / 1 3 7 7 2	国際出願日 (日.月.年) 2 8 . 1 0 . 0 3	優先日 (日.月.年) 3 0 . 1 0 . 0 2
国際特許分類 (IPC) Int. Cl. H 0 4 N 1 / 3 8 7		
出願人 (氏名又は名称) 独立行政法人科学技術振興機構		

1. この報告書は、PCT35条に基づきこの国際予備審査機関で作成された国際予備審査報告である。
法施行規則第57条 (PCT36条) の規定に従い送付する。

2. この国際予備審査報告は、この表紙を含めて全部で 3 ページからなる。

3. この報告には次の附属物件も添付されている。

a ☒ 附属書類は全部で 1 2 ページである。

☒ 補正されて、この報告の基礎とされた及び/又はこの国際予備審査機関が認めた訂正を含む明細書、請求の範囲及び/又は図面の用紙 (PCT規則70.16及び実施細則第607号参照)

☐ 第I欄4. 及び補充欄に示したように、出願時における国際出願の開示の範囲を超えた補正を含むものとこの国際予備審査機関が認定した差替え用紙

b ☐ 電子媒体は全部で (電子媒体の種類、数を示す)。
配列表に関する補充欄に示すように、コンピュータ読み取り可能な形式による配列表又は配列表に関連するテーブルを含む。(実施細則第802号参照)

4. この国際予備審査報告は、次の内容を含む。

☒ 第I欄 国際予備審査報告の基礎

☐ 第II欄 優先権

☐ 第III欄 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成

☐ 第IV欄 発明の単一性の欠如

☒ 第V欄 PCT35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明

☐ 第VI欄 ある種の引用文献

☐ 第VII欄 国際出願の不備

☐ 第VIII欄 国際出願に対する意見

国際予備審査の請求書を受理した日
2 6 . 0 5 . 2 0 0 4

国際予備審査報告を作成した日
1 8 . 1 1 . 2 0 0 4

名称及びあて先
日本国特許庁 (IPEA/J P)
郵便番号 1 0 0 - 8 9 1 5
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

5 V

3 3 5 9

仲間 晃

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 7 1

様式PCT/IPEA/409 (表紙) (2004年1月)

Best Available Copy

第I欄 報告の基礎

1. この国際予備審査報告は、下記に示す場合を除くほか、国際出願の言語を基礎とした。

☐ この報告は、_____ 語による翻訳文を基礎とした。

それは、次の目的で提出された翻訳文の言語である。

- ☐ PCT規則12.3及び23.1(b)にいう国際調査
☐ PCT規則12.4にいう国際公開
☐ PCT規則55.2又は55.3にいう国際予備審査

2. この報告は下記の出願書類を基礎とした。(法第6条(PCT14条)の規定に基づく命令に応答するために提出された差替え用紙は、この報告において「出願時」とし、この報告に添付していない。)

☐ 出願時の国際出願書類

☒ 明細書

第 1-26 ページ、出願時に提出されたもの

第 _____ ページ*、 _____ 付で国際予備審査機関が受理したもの

第 _____ ページ*、 _____ 付で国際予備審査機関が受理したもの

☒ 請求の範囲

第 4-14 項、出願時に提出されたもの

第 _____ 項*、PCT19条の規定に基づき補正されたもの

第 1-3、15-20 項*、26.05.2004 付で国際予備審査機関が受理したもの

第 _____ 項*、 _____ 付で国際予備審査機関が受理したもの

☒ 図面

第 1-13 ページ/図、出願時に提出されたもの

第 _____ ページ/図*、 _____ 付で国際予備審査機関が受理したもの

第 _____ ページ/図*、 _____ 付で国際予備審査機関が受理したもの

☐ 配列表又は関連するテーブル

配列表に関する補充欄を参照すること。

3. ☐ 補正により、下記の書類が削除された。

- ☐ 明細書 第 _____ ページ
☐ 請求の範囲 第 _____ 項
☐ 図面 第 _____ ページ/図
☐ 配列表(具体的に記載すること) _____
☐ 配列表に関連するテーブル(具体的に記載すること) _____

4. ☐ この報告は、補充欄に示したように、この報告に添付されかつ以下に示した補正が出願時における開示の範囲を超えてされたものと認められるので、その補正がされなかったものとして作成した。(PCT規則70.2(c))

- ☐ 明細書 第 _____ ページ
☐ 請求の範囲 第 _____ 項
☐ 図面 第 _____ ページ/図
☐ 配列表(具体的に記載すること) _____
☐ 配列表に関連するテーブル(具体的に記載すること) _____

* 4. に該当する場合、その用紙に“superseded”と記入されることがある。

第V欄 新規性、進歩性又は産業上の利用可能性についての法第12条（PCT35条(2)）に定める見解、それを裏付ける文献及び説明

1. 見解

新規性 (N)	請求の範囲	1-20	有 無
	請求の範囲		
進歩性 (IS)	請求の範囲	1-20	有 無
	請求の範囲		
産業上の利用可能性 (IA)	請求の範囲	1-20	有 無
	請求の範囲		

2. 文献及び説明 (PCT規則70.7)

文献1：田森秀明他，数論変換を用いた改ざん検出可能な電子透かし方式，電子情報通信学会技術研究報告 IE2001-33，2001.07.01，p. 105-110

文献2：田森秀明他，数論変換による脆弱型電子透かしを用いた静止画像の改ざん位置検出可能と改ざん訂正，電子情報通信学会技術研究報告 IE2002-45，2002.07.01，p. 19-24

国際調査報告で引用された文献1及び2のいずれにも、埋め込み位置の原画像ブロックの数論変換ブロックと署名画像の画素値と埋め込み強度から埋め込み量を求めること、及び周囲の所定のブロックの情報をパラメータとしたランダム化関数に基づいて署名画像の埋め込み位置に対応する抽出位置を求めること、については記載されておらず、当業者にとって自明なものでもない。
よって、請求の範囲1-20に係る発明は、新規性、進歩性を有するものである。

請 求 の 範 囲

1. (補正後) 処理部は、数論変換のパラメータである法 P 、2以上の偶数である位数 N 、根 α を設定するステップと、

5 処理部は、記憶部から、埋め込み対象の原画像 $[f]$ をブロック分割した原画像ブロック $f_{i,j}(x,y)$ を読み込むステップと、

処理部は、設定された法 P 、位数 N 、根 α を用いて、原画像ブロック $f_{i,j}(x,y)$ を数論変換して原画像ブロックの数論変換ブロック $F_{i,j}(x,y)$ を計算するステップと、

10 処理部は、各ブロックにおける署名画像の埋め込み位置 (x', y') を、左隣、右隣又は周囲の所定ブロックの情報をパラメータとした所定のランダム化関数に基づき決定するステップと、

処理部は、埋め込むための署名画像の画素値 $g_{i,j}$ を記憶部から読み込むステップと、

15 処理部は、埋め込み位置の原画像ブロックの数論変換ブロック $F_{i,j}(x', y')$ と署名画像の画素値 $g_{i,j}$ と埋め込み強度 ε より、 $F_{i,j}(x', y') + \delta = g_{i,j} \pmod{\varepsilon}$ を満たす絶対値が最小の整数を各ブロックの埋め込み量 δ として求めるステップと、

20 処理部は、原画像ブロックの数論変換ブロック $F_{i,j}(x,y)$ に、 (x,y) に応じて埋め込み量 δ を加算又は減算して、埋め込み済み画像ブロックの数論変換ブロック $H_{i,j}(x,y)$ を求めるステップと、

処理部は、数論変換ブロック $H_{i,j}(x,y)$ の逆数論変換を計算して、埋め込み済み画像ブロック $h_{i,j}(x,y)$ を求めるステップと、

25 処理部は、全ての (i, j) ブロックについて埋め込み済み画像ブロック $h_{i,j}(x,y)$ を求めることにより埋め込み済み画像 $[h]$ を得て、それを記憶部に記憶する、及び／又は、出力部若しくはインターフェースにより出力するステップとを含む改ざん検出方法。

2. (補正後) 処理部は、埋め込み済み画像[h]をブロック分割した埋め込み済み画像ブロック $h_{i,j}(x,y)$ を、記憶部又は入力部又はインターフェースから読み込むステップと、

処理部は、数論変換のためのパラメータである法P、2以上の偶数である位数

5 N、根 α を設定するステップと、

処理部は、埋め込み済み画像ブロック $h_{i,j}(x,y)$ を数論変換して埋め込み済み画像ブロックの数論変換ブロック $H_{i,j}(x,y)$ を計算するステップと、

処理部は、署名画像の埋め込み位置に対応する抽出位置 (x',y') を、左隣、右隣又は周囲の所定ブロックの情報をパラメータとした所定のランダム化関数
10 に基づいて決定するステップと、

処理部は、抽出位置の数論変換ブロック $H_{i,j}(x',y')$ の埋め込み強度 ε による剰余を取ることによって、署名画像の画素値 $g_{i,j}$ を抽出するステップと、

処理部は、全ての (i,j) ブロックについて署名画像の画素値 $g_{i,j}$ を求めることにより署名画像[g]を得て、それを記憶部に記憶する、及び／又は、表示部若しくは出力部若しくはインターフェースに出力するステップと
15 を含む改ざん検出方法。

3. (補正後) 署名画像を原画像に埋め込む処理及び署名画像を抽出する処理を含む改ざん検出方法であって、

20 前記埋め込む処理は、

処理部は、数論変換のパラメータである法P、2以上の偶数である位数N、根 α を設定するステップと、

処理部は、記憶部から、埋め込み対象の原画像[f]をブロック分割した原画像ブロック $f_{i,j}(x,y)$ を読み込むステップと、

25 処理部は、設定された法P、位数N、根 α を用いて、原画像ブロック $f_{i,j}(x,y)$ を数論変換して原画像ブロックの数論変換ブロック $F_{i,j}(x,y)$ を計算するステップと、

処理部は、各ブロックにおける署名画像の埋め込み位置 (x',y') を、左隣、

右隣又は周囲の所定ブロックの情報をパラメータとした所定のランダム化関数に基づき決定するステップと、

処理部は、埋め込むための署名画像の画素値 $g_{i,j}$ を記憶部から読み込むステップと、

- 5 処理部は、埋め込み位置の原画像ブロックの数論変換ブロック $F_{i,j}(x', y')$ と署名画像の画素値 $g_{i,j}$ と埋め込み強度 ε により、 $F_{i,j}(x', y') + \delta = g_{i,j} \pmod{\varepsilon}$ を満たす絶対値が最小の整数を各ブロックの埋め込み量 δ として求めるステップと、

- 10 処理部は、原画像ブロックの数論変換ブロック $F_{i,j}(x, y)$ に、 (x, y) に応じて埋め込み量 δ を加算又は減算して、埋め込み済み画像ブロックの数論変換ブロック $H_{i,j}(x, y)$ を求めるステップと、

処理部は、数論変換ブロック $H_{i,j}(x, y)$ の逆数論変換を計算して、埋め込み済み画像ブロック $h_{i,j}(x, y)$ を求めるステップと、

- 15 処理部は、全ての (i, j) ブロックについて埋め込み済み画像ブロック $h_{i,j}(x, y)$ を求めることにより埋め込み済み画像 $[h]$ を得て、それを記憶部に記憶する、及び／又は、出力部若しくはインターフェースにより出力するステップとを含み、

前記抽出処理は、

- 20 処理部は、埋め込み済み画像 $[h]$ をブロック分割した埋め込み済み画像ブロック $h_{i,j}(x, y)$ を、記憶部又は入力部又はインターフェースから読み込むステップと、

処理部は、数論変換のためのパラメータである法 P 、2以上の偶数である位数 N 、根 α を設定するステップと、

- 25 処理部は、埋め込み済み画像ブロック $h_{i,j}(x, y)$ を数論変換して埋め込み済み画像ブロックの数論変換ブロック $H_{i,j}(x, y)$ を計算するステップと、

処理部は、署名画像の埋め込み位置に対応する抽出位置 (x', y') を、左隣、右隣又は周囲の所定ブロックの情報をパラメータとした所定のランダム化関数に基づいて決定するステップと、

処理部は、抽出位置の数論変換ブロック $H_{i,j}(x', y')$ の埋め込み強度 ε による剰余を取ることによって、署名画像の画素値 $g_{i,j}$ を抽出するステップと、

処理部は、全ての (i, j) ブロックについて署名画像の画素値 $g_{i,j}$ を求めることにより署名画像 $[g]$ を得て、それを記憶部に記憶する、及び／又は、表示部若しくは出力部若しくはインターフェースに出力するステップとを含む改ざん検出方法。

4. 処理部は、出力部又はインターフェースを介して、抽出側装置に、法 P 及び埋め込み済み画像 $[h]$ を、また、必要に応じて位数 N を送信するステップをさらに含む請求項1または3に記載の改ざん検出方法。

5. 処理部は、数論変換のためのパラメータである法 P と埋め込み済み画像 $[h]$ 、必要に応じて N を送信側装置から受信するステップをさらに含む請求項2又は3に記載の改ざん検出方法。

6. 処理部は、埋め込み済み画像 $[h]$ 及び署名画像 $[g]$ に基づいて、原画像 $[f]$ を求めるステップをさらに含む請求項1乃至3のいずれかに記載の改ざん検出方法。

7. P は、素数のべき乗による任意の合成数であることを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方法。

8. N は、署名画像の埋め込み側及び抽出側で共通にあらかじめ記憶部に記憶してあること、又は、埋め込み側から抽出側へ伝送されることを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方法。

9. 処理部は、 $N \mid \text{GCD}[(p_1 - 1), (p_2 - 1), \dots, (p_m - 1)]$ により求められた位数 N の候補から、予め定められた優先順位でいずれかの位数 N を選択することを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方法。

10. 処理部は、設定された法 P 及び位数 N に基づき、一意に算出される中国剰余定理等の予め定められた式により根 α を計算することを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方法。

5

11. 処理部は、 p_i を素数、 r_i を正の整数として、 $P=p_1^{r_1}p_2^{r_2}\cdots p_m^{r_m}$ で表されるとした P を設定し、

処理部は、位数 N を、 $N \mid \text{GCD}[(p_1-1), (p_2-1), \dots, (p_m-1)]$ を満たす正の整数から選択し、又は、記憶部から読み取り、

10

処理部は、 p_i を法とする位数 N の根 $\alpha_{1,i}$ を計算し、

処理部は、 $p_i^{r_i}$ を法とする位数 N の根 $\alpha_{2,i}$ を、 $\alpha_{1,i}$ より求め、

処理部は、中国剰余定理により、 P を法とする位数 N の根 α を、 $\alpha_{2,i}$ より求める

ことを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方法。

15

12. 処理部は、 P 、 N 及び α を用いて、次式により $x(n)$ と $X(k)$ との間の数論変換を実行することを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方法。

$$X(k) = \sum_{n=0}^{N-1} x(n) \alpha^{kn} \pmod{P} \quad (1)$$

$$x(n) = N^{-1} \sum_{k=0}^{N-1} X(k) \alpha^{-kn} \pmod{P} \quad (2)$$

- 20 (ここに、 P (素数のべき乗となる任意の合成数)、 α 、(を正の整数、 N を $\alpha^N=1 \pmod{P}$ となる最小の正の整数)

$$X=[T]x$$

$$x=[T]^{-1}X$$

($[T]$: 変換行列、 $[T]^{-1}$: 逆変換行列)

13. 前記ランダム化関数は、法Pの値、及び／又は、隣接するブロック若しくは埋め込み処理で変更されない所定ブロックの画素値をパラメータとし、位置を一意に決定する関数であることを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方法。

14. 前記ランダム化関数は、以下の式による関数であることを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方法。

$$x' = r_{x'}(P, i, j, f_{i,l}(0, 0)) \quad (10)$$

$$y' = r_{y'}(P, i, j, f_{i,l}(0, 0)) \quad (11)$$

$$l = j - 1 \pmod{L} \quad (12)$$

15. (補正後) 処理部は、数論変換のパラメータである法P、2以上の偶数である位数N、根 α を設定するステップと、

処理部は、記憶部から、埋め込み対象の原画像[f]をブロック分割した原画像ブロック $f_{i,j}(x, y)$ を読み込むステップと、

処理部は、設定された法P、位数N、根 α を用いて、原画像ブロック $f_{i,j}(x, y)$ を数論変換して原画像ブロックの数論変換ブロック $F_{i,j}(x, y)$ を計算するステップと、

処理部は、各ブロックにおける署名画像の埋め込み位置 (x', y') を、左隣、右隣又は周囲の所定ブロックの情報をパラメータとした所定のランダム化関数に基づき決定するステップと、

処理部は、埋め込むための署名画像の画素値 $g_{i,j}$ を記憶部から読み込むステップと、

処理部は、埋め込み位置の原画像ブロックの数論変換ブロック $F_{i,j}(x', y')$ と署名画像の画素値 $g_{i,j}$ と埋め込み強度 ε より、

$F_{i,j}(x', y') + \delta = g_{i,j} \pmod{\varepsilon}$ を満たす絶対値が最小の整数を各ブロックの埋め込み量 δ として求めるステップと、

処理部は、原画像ブロックの数論変換ブロック $F_{i,j}(x,y)$ に、 (x,y) に応じて埋め込み量 δ を加算又は減算して、埋め込み済み画像ブロックの数論変換ブロック $H_{i,j}(x,y)$ を求めるステップと、

5 処理部は、数論変換ブロック $H_{i,j}(x,y)$ の逆数論変換を計算して、埋め込み済み画像ブロック $h_{i,j}(x,y)$ を求めるステップと、

処理部は、全ての (i,j) ブロックについて埋め込み済み画像ブロック $h_{i,j}(x,y)$ を求めることにより埋め込み済み画像 $[h]$ を得て、それを記憶部に記憶する、及び／又は、出力部若しくはインターフェースにより出力するステップと

をコンピュータに実行させるための改ざん検出プログラム。

10

16. (補正後) 処理部は、埋め込み済み画像 $[h]$ をブロック分割した埋め込み済み画像ブロック $h_{i,j}(x,y)$ を、記憶部又は入力部又はインターフェースから読み込むステップと、

15 処理部は、数論変換のためのパラメータである法 P 、2以上の偶数である位数 N 、根 α を設定するステップと、

処理部は、埋め込み済み画像ブロック $h_{i,j}(x,y)$ を数論変換して埋め込み済み画像ブロックの数論変換ブロック $H_{i,j}(x,y)$ を計算するステップと、

20 処理部は、署名画像の埋め込み位置に対応する抽出位置 (x',y') を、左隣、右隣又は周囲の所定ブロックの情報をパラメータとした所定のランダム化関数に基づいて決定するステップと、

処理部は、抽出位置の数論変換ブロック $H_{i,j}(x',y')$ の埋め込み強度 ε による剰余を取ることによって、署名画像の画素値 $g_{i,j}$ を抽出するステップと、

25 処理部は、全ての (i,j) ブロックについて署名画像の画素値 $g_{i,j}$ を求めることにより署名画像 $[g]$ を得て、それを記憶部に記憶する、及び／又は、表示部若しくは出力部若しくはインターフェースに出力するステップと

をコンピュータに実行させるための改ざん検出プログラム。

17. (補正後) 署名画像を原画像に埋め込む処理及び署名画像を抽出する処理をコンピュータに実行させるための改ざん検出プログラムであって、

前記埋め込む処理は、

5 処理部は、数論変換のパラメータである法 P 、2以上の偶数である位数 N 、根 α を設定するステップと、

処理部は、記憶部から、埋め込み対象の原画像 $[f]$ をブロック分割した原画像ブロック $f_{i,j}(x,y)$ を読み込むステップと、

10 処理部は、設定された法 P 、位数 N 、根 α を用いて、原画像ブロック $f_{i,j}(x,y)$ を数論変換して原画像ブロックの数論変換ブロック $F_{i,j}(x,y)$ を計算するステップと、

処理部は、各ブロックにおける署名画像の埋め込み位置 (x', y') を、左隣、右隣又は周囲の所定ブロックの情報をパラメータとした所定のランダム化関数に基づき決定するステップと、

15 処理部は、埋め込むための署名画像の画素値 $g_{i,j}$ を記憶部から読み込むステップと、

処理部は、埋め込み位置の原画像ブロックの数論変換ブロック $F_{i,j}(x', y')$ と署名画像の画素値 $g_{i,j}$ と埋め込み強度 ε により、 $F_{i,j}(x', y') + \delta = g_{i,j} \pmod{\varepsilon}$ を満たす絶対値が最小の整数を各ブロックの埋め込み量 δ として求めるステップと、

20 処理部は、原画像ブロックの数論変換ブロック $F_{i,j}(x,y)$ に、 (x,y) に応じて埋め込み量 δ を加算又は減算して、埋め込み済み画像ブロックの数論変換ブロック $H_{i,j}(x,y)$ を求めるステップと、

処理部は、数論変換ブロック $H_{i,j}(x,y)$ の逆数論変換を計算して、埋め込み済み画像ブロック $h_{i,j}(x,y)$ を求めるステップと、

25 処理部は、全ての (i,j) ブロックについて埋め込み済み画像ブロック $h_{i,j}(x,y)$ を求めることにより埋め込み済み画像 $[h]$ を得て、それを記憶部に記憶する、及び／又は、出力部若しくはインターフェースにより出力するステップとを含み、

前記抽出処理は、

処理部は、埋め込み済み画像[h]をブロック分割した埋め込み済み画像ブロック $h_{i,j}(x,y)$ を、記憶部又は入力部又はインターフェースから読み込むステップと、

5 処理部は、数論変換のためのパラメータである法P、2以上の偶数である位数N、根 α を設定するステップと、

処理部は、埋め込み済み画像ブロック $h_{i,j}(x,y)$ を数論変換して埋め込み済み画像ブロックの数論変換ブロック $H_{i,j}(x,y)$ を計算するステップと、

10 処理部は、署名画像の埋め込み位置に対応する抽出位置 (x', y') を、左隣、右隣又は周囲の所定ブロックの情報をパラメータとした所定のランダム化関数に基づいて決定するステップと、

処理部は、抽出位置の数論変換ブロック $H_{i,j}(x', y')$ の埋め込み強度 ε による剰余を取ることによって、署名画像の画素値 $g_{i,j}$ を抽出するステップと、

15 処理部は、全ての (i, j) ブロックについて署名画像の画素値 $g_{i,j}$ を求めることにより署名画像[g]を得て、それを記憶部に記憶する、及び／又は、表示部若しくは出力部若しくはインターフェースに出力するステップと

をコンピュータに実行させるための改ざん検出プログラム。

18. (補正後) 処理部は、数論変換のパラメータである法P、2以上の偶数である位数N、根 α を設定するステップと、

20 処理部は、記憶部から、埋め込み対象の原画像[f]をブロック分割した原画像ブロック $f_{i,j}(x,y)$ を読み込むステップと、

処理部は、設定された法P、位数N、根 α を用いて、原画像ブロック $f_{i,j}(x,y)$ を数論変換して原画像ブロックの数論変換ブロック $F_{i,j}(x,y)$ を計算するステップと、

25 処理部は、各ブロックにおける署名画像の埋め込み位置 (x', y') を、左隣、右隣又は周囲の所定ブロックの情報をパラメータとした所定のランダム化関数に基づき決定するステップと、

処理部は、埋め込むための署名画像の画素値 $g_{i,j}$ を記憶部から読み込むステ

ップと、

処理部は、埋め込み位置の原画像ブロックの数論変換ブロック $F_{i,j}(x', y')$ と署名画像の画素値 $g_{i,j}$ と埋め込み強度 ε より、

5 $F_{i,j}(x', y') + \delta = g_{i,j} \pmod{\varepsilon}$ を満たす絶対値が最小の整数を各ブロックの埋め込み量 δ として求めるステップと、

処理部は、原画像ブロックの数論変換ブロック $F_{i,j}(x, y)$ に、 (x, y) に応じて埋め込み量 δ を加算又は減算して、埋め込み済み画像ブロックの数論変換ブロック $H_{i,j}(x, y)$ を求めるステップと、

10 処理部は、数論変換ブロック $H_{i,j}(x, y)$ の逆数論変換を計算して、埋め込み済み画像ブロック $h_{i,j}(x, y)$ を求めるステップと、

処理部は、全ての (i, j) ブロックについて埋め込み済み画像ブロック $h_{i,j}(x, y)$ を求めることにより埋め込み済み画像 $[h]$ を得て、それを記憶部に記憶する、及び／又は、出力部若しくはインターフェースにより出力するステップと

をコンピュータに実行させるための改ざん検出プログラムを記録した記録媒体。

15

19. (補正後) 処理部は、埋め込み済み画像 $[h]$ をブロック分割した埋め込み済み画像ブロック $h_{i,j}(x, y)$ を、記憶部又は入力部又はインターフェースから読み込むステップと、

20 処理部は、数論変換のためのパラメータである法 P 、2以上の偶数である位数 N 、根 α を設定するステップと、

処理部は、埋め込み済み画像ブロック $h_{i,j}(x, y)$ を数論変換して埋め込み済み画像ブロックの数論変換ブロック $H_{i,j}(x, y)$ を計算するステップと、

25 処理部は、署名画像の埋め込み位置に対応する抽出位置 (x', y') を、左隣、右隣又は周囲の所定ブロックの情報をパラメータとした所定のランダム化関数に基づいて決定するステップと、

処理部は、抽出位置の数論変換ブロック $H_{i,j}(x', y')$ の埋め込み強度 ε による剰余を取ることによって、署名画像の画素値 $g_{i,j}$ を抽出するステップと、

処理部は、全ての (i, j) ブロックについて署名画像の画素値 $g_{i,j}$ を求めることに

より署名画像[g]を得て、それを記憶部に記憶する、及び／又は、表示部若しくは出力部若しくはインターフェースに出力するステップと

をコンピュータに実行させるための改ざん検出プログラムを記録した記録媒体。

- 5 20. (補正後) 署名画像を原画像に埋め込む処理及び署名画像を抽出する処理をコンピュータに実行させるための改ざん検出プログラムを記録した記録媒体であって、

前記埋め込む処理は、

- 10 処理部は、数論変換のパラメータである法P、2以上の偶数である位数N、根 α を設定するステップと、

処理部は、記憶部から、埋め込み対象の原画像[f]をブロック分割した原画像ブロック $f_{i,j}(x,y)$ を読み込むステップと、

- 15 処理部は、設定された法P、位数N、根 α を用いて、原画像ブロック $f_{i,j}(x,y)$ を数論変換して原画像ブロックの数論変換ブロック $F_{i,j}(x,y)$ を計算するステップと、

処理部は、各ブロックにおける署名画像の埋め込み位置 (x',y') を、左隣、右隣又は周囲の所定ブロックの情報をパラメータとした所定のランダム化関数に基づき決定するステップと、

- 20 処理部は、埋め込むための署名画像の画素値 $g_{i,j}$ を記憶部から読み込むステップと、

処理部は、埋め込み位置の原画像ブロックの数論変換ブロック $F_{i,j}(x',y')$ と署名画像の画素値 $g_{i,j}$ と埋め込み強度 ε により、 $F_{i,j}(x',y') + \delta = g_{i,j} \pmod{\varepsilon}$ を満たす絶対値が最小の整数を各ブロックの埋め込み量 δ として求めるステップと、

- 25 処理部は、原画像ブロックの数論変換ブロック $F_{i,j}(x,y)$ に、 (x,y) に応じて埋め込み量 δ を加算又は減算して、埋め込み済み画像ブロックの数論変換ブロック $H_{i,j}(x,y)$ を求めるステップと、

処理部は、数論変換ブロック $H_{i,j}(x,y)$ の逆数論変換を計算して、埋め込み済み画像ブロック $h_{i,j}(x,y)$ を求めるステップと、

処理部は、全ての (i, j) ブロックについて埋め込み済み画像ブロック $h_{i,j}(x, y)$ を求めることにより埋め込み済み画像 $[h]$ を得て、それを記憶部に記憶する、及び／又は、出力部若しくはインターフェースにより出力するステップとを含み、

5 前記抽出処理は、

処理部は、埋め込み済み画像 $[h]$ をブロック分割した埋め込み済み画像ブロック $h_{i,j}(x, y)$ を、記憶部又は入力部又はインターフェースから読み込むステップと、

10 処理部は、数論変換のためのパラメータである法 P 、2以上の偶数である位数 N 、根 α を設定するステップと、

処理部は、埋め込み済み画像ブロック $h_{i,j}(x, y)$ を数論変換して埋め込み済み画像ブロックの数論変換ブロック $H_{i,j}(x, y)$ を計算するステップと、

15 処理部は、署名画像の埋め込み位置に対応する抽出位置 (x', y') を、左隣、右隣又は周囲の所定ブロックの情報をパラメータとした所定のランダム化関数に基づいて決定するステップと、

処理部は、抽出位置の数論変換ブロック $H_{i,j}(x', y')$ の埋め込み強度 ε による剰余を取ることによって、署名画像の画素値 $g_{i,j}$ を抽出するステップと、

20 処理部は、全ての (i, j) ブロックについて署名画像の画素値 $g_{i,j}$ を求めることにより署名画像 $[g]$ を得て、それを記憶部に記憶する、及び／又は、表示部若しくは出力部若しくはインターフェースに出力するステップと

をコンピュータに実行させるための改ざん検出プログラムを記録した記録媒体。